CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research elaborates about the pro-Palestinian hacktivist group "Dark Storm" which claimed the large-scale DDoS attack against X (formerly Twitter). The attack disrupted access to the platform, causing outages for users worldwide. Recently, Dark Storm was also targeting Western organizations and critical infrastructure in the US, Israel, Ukraine, and the UAE.
- Kansas-based healthcare provider, Sunflower Medical Group, has suffered a data breach that potentially exposed sensitive patient information. The breach, which occurred in December 2024 and was disclosed this week, compromised the data of nearly 221,000 patients. The affected information potentially had patients' names, addresses, dates of birth, Social Security numbers, driver's license numbers, medical information, and health insurance information.
- Turkish internet service provider, TurkNet, reported it has fallen victim to a cyberattack. The threat actors have reportedly attempted to extort 3 Bitcoins in ransom in exchange for the approximately 1.5 million customers' personal data. The personal data included full names, national ID numbers, phone numbers, addresses, subscription details and static IP addresses.
- Brydens Lawyers, a major Australian law firm, has reportedly experienced a ransomware attack. The attack compromised 600GB of sensitive client data, including case, client, and staff data, however no threat actor claimed responsibility.
- The Federated States of Micronesia's health system has fallen victim to a ransomware attack, causing operational disruptions. The attack forced hospital and clinic staff to revert to manual record-keeping, while authorities work to contain the breach and restore affected systems.
- A cyberattack has disrupted payment systems at Spar supermarkets across Switzerland, causing outages that prevent customers from using card payments. The company said its IT systems were compromised, and operations are currently disrupted, raising supply chain and food stock concerns.
- The Pelham School District in New Hampshire was rendered offline following a cyberattack that disrupted its IT infrastructure. The district has suspended access to critical online services while cybersecurity teams work to restore operations and assess the breach's impact.
- Edesur Dominicana, a power distribution company in the Dominican Republic, has confirmed a cyberattack on its systems. While the company stated that no customer data was leaked, the attack caused service disruptions and forced IT teams to implement emergency response measures.
- New Zealand's Vercoe Insurance Brokers has fallen victim to a cyberattack, resulting in operational downtime and potential data exposure. The firm has not disclosed the full extent of the breach, but clients have been advised to remain vigilant for potential fraud attempts.

VULNERABILITIES AND PATCHES

- Microsoft's March 2025 Patch Tuesday has addressed 57 flaws, including 6 critical vulnerabilities across its products. The update includes fixes in product families ranging from Windows to .NET, with various vulnerabilities including code execution, elevated privilege, disclosure of information, denial of service, and security feature bypass being addressed.
- Researchers have identified a 0-day vulnerability (CVE-2025-24983) being used in targeted cyber espionage campaigns. The vulnerability allows attackers to execute remote code on compromised systems and was patched in Microsoft's latest security update.
- Hackers are actively exploiting a vulnerability in a font-rendering library used by Facebook. The flaw allows attackers to run malicious code by tricking users into opening compromised files. Researchers warn that this vulnerability is being used in phishing campaigns to distribute malware.
- Researchers warn of a set of 29 undocumented commands in Chinese manufacturer Espressif's ESP32 Bluetooth chip, which is used in more than 1 billion IoT devices worldwide. This set of commands collectively assigned CVE-2025-27840, could allow spoofing and establishing persistence, and is particularly concerning due to the prevalence of the ESP32 chips.

THREAT INTELLIGENCE REPORTS

- Check Point Research has uncovered a new campaign by the Blind Eagle APT group, which has been targeting organizations and government institutions in Colombia. The group, known for its sophisticated phishing techniques, has been exploiting vulnerability CVE-2024-43451 to distribute known malware like Remcos RAT, and infiltrate government and financial institutions.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(Exploit.Wins.CVE-2024-43451.ta.A, Infostealer.Win.Generic.F, Injector.Win.RunPE.A, Infostealer.Win.PasswordStealer.A, Trojan.Win.Unpacme.gl.I, Exploit.Win.UnDefender.A, Packer.Win.VBNetCrypter.H, Packer.Win.DotNetCrypter.G, Trojan.Win.Benjaminbo_test.gl.A, behavioral.win.suspautorun.a, behavioral.win.imagemodification.g)*

- Check Point Research has released February 2025's Most Wanted Malware report, highlighting AsyncRAT as a top emerging threat. The malware is increasingly being used to target trusted platforms, leveraging obfuscation techniques to avoid detection. The RAT enables remote control and data exfiltration.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(RAT.Wins.AsyncRAT.*)*

- Mandiant researchers have identified a China-linked cyber espionage campaign targeting Juniper routers. The threat actor group, UNC3886, is exploiting vulnerabilities in unpatched devices to establish persistent access for intelligence gathering.
- Microsoft has warned of an ongoing phishing campaign impersonating Booking.com. The campaign delivers a suite of credential-stealing malware, aiming to compromise user accounts. The attackers use highly convincing emails mimicking legitimate Booking.com messages to deceive victims.